Prevenir

Aprender

Proteger

CIBERAPP

Uso seguro de Internet
Guía para padres y educadores

Programa integral de prevención primaria de la ciberviolencia en menores de la provincia de Alicante

CRÍMINA
Centro para el estudio y prevención de la delincuencia

UNIVERSITAS Miguel Hernández

DIPUTACIÓN DE ALICANTE

CIBERAPP

Aprender
Prevenir
Proteger

Edita Excma. Diputación Provincial de Alicante (Área de Igualdad y Juventud)
Autores Fernando Miró Llinares (Director Centro Crímina), Natalia García Guilabert, Teresa Díez Ros, Nuria Rodríguez Gómez
Diseño e Impresión Puntual
Depósito legal A 808-2014
Alicante, 2014

> ÍNDICE

INTERNET ES SEGURO

¿Es seguro Internet? ¿Lo es la ciudad en la que vivimos? ¿Y Alicante, Madrid, Londres, Sao Paulo o Nueva York, son seguras? Internet es, para muchos padres y educadores, como una ciudad en la que no hemos estado nunca, como un lugar extraño que no conocemos, al que nos acercamos por primera vez y que nos produce cierta inseguridad por no haber estado allí antes. Es cierto, y ello se verá en esta "guía", que en el ciberespacio hay amenazas, pero también puede haberlas en las ciudades y pueblos por los que caminamos sin temor cuando ya hemos estado en ellos, cuando los conocemos y comprendemos cómo son, por dónde podemos ir, cómo debemos actuar.

Internet, además, ha venido para quedarse. En él ya vivimos gran parte de nuestro tiempo muchos adultos, y mucho más lo hacen los menores que transitan diariamente por él contactando con sus compañeros, haciendo nuevos amigos, compartiendo información y experiencias. Y pese a que se desenvuelvan los menores por Internet con aparente soltura, especialmente si la comparamos con la torpeza técnica con la que lo hacemos muchos adultos que no nacimos con la existencia de ese mundo digital, eso no significa que conozcan esa ciudad, ese lugar nuevo por el que caminan. Pues Internet no es sólo un entorno técnico, sino básicamente un entorno de relaciones personales, para lo cual los adultos estamos mucho más preparados que los menores: ya las hemos vivido, ya tenemos experiencias y podemos explicarlas a los que se inician en el mundo.

¿Caminan entonces nuestros hijos, nuestros alumnos, por un lugar peligroso cuando están en Internet? No especialmente, pero sí caminan por un lugar nuevo que no comprenden del todo y al que les podemos ayudar a conocer si nosotros, padres y educadores, también lo comprendemos. Así, debemos comprender que lo peligroso no es que los menores accedan al ciberespacio sino lo que hacen dentro de él; debemos entender, y hacerles comprender, los riesgos que conlleva realizar determinadas acciones; y debemos seguir explicándoles como funcionan las relaciones sociales y personales tanto en el mundo físico como en Internet.

Esta guía, pues, pretende ser como un pequeño mapa de un lugar nuevo, como una guía que nos señale las amenazas, que nos advierta como no transitarlas, que nos ayude a prevenirlas y a tratarlas. También busca desdramatizar la visión de Internet como un lugar peligroso o como un lugar para el que "los mayores" no estamos preparados: lo estamos aún más que aquellos que, con nuestra ayuda, pronto pasarán por todas las esquinas de ese nuevo lugar que no debe asustarnos si empezamos a conocerlo.

CIBERAPP
Guía para padres y educadores

"Aprender para saber prevenir y para poder proteger"

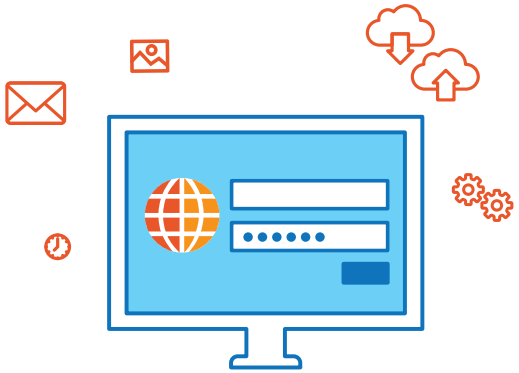
La **Guía CiberApp** se basa en los datos científicos recogidos a través del estudio realizado por la Diputación Provincial de Alicante y el Centro Crímina de la Universidad Miguel Hernández de Elche.

El objetivo de dicho estudio era conocer y comprender el alcance de la cibercriminalidad contra los menores alicantinos y su relación con las actividades cotidianas que éstos realizan en el ciberespacio. Para ello, se encuestó a una muestra de 2.038 menores alicantinos, de edades comprendidas entre los 12 y los 18 años, en 20 institutos de la provincia seleccionados de forma aleatoria.

La investigación reveló que más del 50% de los menores encuestados, había sufrido algún tipo de agresión a través de Internet, desde insultos y amenazas hasta acoso sexual. Las conclusiones del estudio las podemos encontrar en este link:

http://issuu.com/diputacionalicante/docs/conclusiones_ciberapp

Los resultados también mostraron que, en la mayoría de ocasiones, esta victimización viene facilitada por los malos hábitos de los menores en el uso de Internet, realizando, sin ser conscientes de ello, conductas de riesgo.



La finalidad de la **Guía CiberApp** es proporcionar **información sobre los riesgos** a los que pueden estar expuestos los menores al hacer un uso no seguro de las nuevas tecnologías, con el objeto de reducir el número de víctimas entre nuestros jóvenes, a través de **tres principios básicos**:

Aprender a identificar conductas amenazantes en el ciberespacio y estrategias frente a ellas.

Prevenir posibles ciberataques contra los menores atendiendo a sus características particulares.

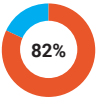
Protegerlos enseñándoles a hacer un uso seguro de Internet.

MENORES Y TIC: LA REALIDAD DEL USO

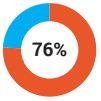
Las Tecnologías de la Información y la Comunicación, conocidas como TIC, es el término que hace referencia a todos los dispositivos y sistemas electrónicos (móviles, ordenadores, tablets, portátiles, etc.) utilizados para el tratamiento de la información, su intercambio y comunicación en la sociedad actual.

Es conveniente conocer qué conductas realizan los menores en Internet y el uso que hacen de las nuevas tecnologías con el fin de prevenir su exposición a posibles riesgos en el ciberespacio.

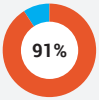
Por tanto, ¿qué uso hacen los menores de las TIC?



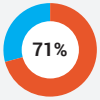
Las conclusiones reveladas en el estudio **CiberApp** en el que se basa esta Guía, reflejan que un **82%** de los menores alicantinos acceden de forma diaria a **Internet a través de su teléfono móvil**. Este hecho corrobora cómo el uso de las TIC está completamente normalizado en la sociedad, especialmente a través de la telefonía móvil.



Los resultados relacionados con el **uso de ordenadores, portátiles o tablets** reflejan que un **76%** de los jóvenes de la provincia, los utilizan diariamente, y sólo el **25%** de ellos comparte estos dispositivos con otras personas, hecho que aumenta la probabilidad de llegar a ser víctima de algún ciberataque.



El **91%** de los menores son usuarios de **redes sociales y de mensajería instantánea**. Casi el 40% de ellos les dedican más de 4 horas diarias.



Respecto al **correo electrónico**, fuente de gran cantidad de ciberataques económicos, el **71%** de los estudiantes alicantinos de edades entre 12 y 18 años, afirman usarlo de forma diaria.

En definitiva, el uso que hacen nuestros menores de las TIC se ha convertido en un hábito implantado y normalizado en su día a día, llegando a ser considerado imprescindible para el desarrollo integral de éste en la sociedad actual.

Es importante conocer las posibilidades que ofrece el ciberespacio para enseñarles a navegar en él de forma segura y adecuada.

LOS MENORES EN INTERNET ESTÁN EXPUESTOS A...

CIBERACOSO

¿Qué es?

El término ciberacoso hace referencia al uso de las TIC por parte de un menor o de un grupo de menores, para acosar de manera repetida e intencional a otro menor.

Puede aparecer en forma de:

Ciberacoso escolar: se refiere a las situaciones de acoso que se producen entre compañeros del colegio a través de las nuevas tecnologías.

Se puede manifestar como una continuación en Internet del acoso que el menor ya sufre en la escuela por parte de sus compañeros o por el contrario, que el acoso se dé únicamente a través de las TIC.

El ciberacoso NO se produce únicamente entre los compañeros del colegio.

El auge de las tecnologías de la comunicación ha hecho que el acoso no se produzca únicamente entre los compañeros del colegio, sino que se extienda a otro grupo de iguales (amigos del barrio, de las actividades extraescolares o incluso de personas conocidas a través de Internet). Al elevar la red de contactos del menor a través del móvil, el ordenador o tablet, las posibilidades de sufrir acoso desde otros ámbitos aumentan.

Se manifiesta…

El ciberacoso puede comprender muchas conductas, desde las burlas, marginación o insultos hasta las amenazas, ridiculizaciones mediante la creación de grupos o páginas dirigidas a ello, clonación de identidades para perjudicar a la víctima o difusión de imágenes manipuladas o comprometidas con el ánimo de dañar.

Es importante saber que…

El modo en que se experimenta el ciberacoso puede tener mayor impacto que el sufrido en el espacio físico, ya que la víctima percibe el ataque de forma continuada (por ejemplo, si un menor recibe una amenaza en el móvil y la lee repetidas veces, la sensación de peligro se percibe de forma más intensa).

Por otra parte, la posibilidad de hacer público el ciberacoso a través de medios como las redes sociales puede incrementar el sentimiento de vergüenza, lo que potencia el daño sufrido por la víctima. Este tipo de plataforma genera también la oportunidad de fomentar que al ataque se sumen nuevos agresores (por ejemplo, cuando se crean grupos en redes sociales o en aplicaciones de mensajería instantánea para burlarse de una persona en particular).

Asimismo, uno de los mayores factores de riesgo de sufrir esta forma de violencia es haber ejercido conductas de acoso a otras personas a través de Internet, especialmente cuando se da entre iguales.

Tenemos que tener en cuenta que cuando este tipo de ataque se realiza de manera puntual, y no continuada, no debemos considerarlo como ciberacoso sino como una ciberagresión aislada, la cual, dependiendo de su gravedad, podrá tener igualmente consecuencias importantes para el menor.

El alcance del fenómeno es…

Aproximadamente el 50% de los menores alicantinos entre 12 y 18 años ha sufrido alguna forma de ciberacoso en algún momento de su vida. Los insultos y la ridiculización son, junto a los rumores y el acceso a cuentas personales sin su consentimiento, los tipos de acoso más sufridos, pues entre un 20 y 23% de los menores han sido víctima de estos ataques.

Las consecuencias son…

El ciberacoso provoca daños psicológicos que pueden afectar al desarrollo psicosocial del menor, generar pérdida de autoestima, ansiedad, estrés, ira o impotencia. La depresión, el desarrollo de fobias, el insomnio o el bajo rendimiento escolar, así como la disminución de la capacidad de concentración son también consecuencias que origina este ciberataque. La gravedad del acoso puede ser distinta según el caso, pero es especialmente problemático cuando se da de forma continua, pública e ilimitada.

Resulta imprescindible atender a los síntomas psicológicos que el menor pueda mostrar para prevenir consecuencias de mayor gravedad.

Los que tienen más riesgo de sufrir estos ataques son…

Los menores que introducen en el ciberespacio facetas de su vida personal y privada, como fotos, vídeos, aficiones, sentimientos, etc., y en especial, aquellos que lo hacen publicándolo en sus perfiles de redes sociales o cediéndoselo a otras personas a través del chat o la mensajería instantánea.

Además, los menores que usan las herramientas de comunicación (redes sociales, blogs, foros, chats, etc.) para cotillear, contactar con desconocidos y molestar o acosar a otros también tienen más riesgo de sufrir este tipo de ciberacoso.

Finalmente, los menores alicantinos que comparten menos tiempo virtual con su padres u otros familiares, es decir, que no son “amigos” en las redes sociales y tampoco comparten con ellos los dispositivos electrónicos (ordenador, tablet, portátil, etc.) tienen más riesgo de ser victimizados.

El menor tiene…

De 12 a 13 años

Los menores alicantinos de esta edad son los que en menor medida sufren este tipo de ataque, pero debemos tener en cuenta que las TIC se usan cada vez a edades más temprana por lo que es importante no subestimar el uso peligroso que pueden hacer de ellas. Tenemos que mantenernos alerta cuando el menor comience a navegar en el ciberespacio o a utilizar el teléfono móvil, debido a que puede ser insultado, marginado o excluido de forma continua, así como ser víctima de falsos rumores especialmente por parte de compañeros del colegio.

De 14 a 15 años

Los insultos repetidos, las amenazas y la ridiculización son las conductas que más sufren los menores de la provincia a esta edad. También es habitual el contacto repetido no deseado, ser víctima de rumores o bulos y el acceso a sus cuentas personales sin su consentimiento.

Los ataques como ser excluido y marginado de forma continua así como la publicación en Internet de fotos o vídeos íntimos, son llevados a cabo, principalmente, por los propios compañeros de clase.

Es importante analizar y conocer cada caso en particular. Para ello debemos favorecer la comunicación con el menor y conocer el uso que hace de las TIC, permitiéndole comunicarse con nosotros en caso de sentirse ciberacosado.

De 16 a 18 años

La conducta más sufrida por los menores alicantinos de esta edad, es el contacto repetido no deseado. Asimismo, estos jóvenes soportan otros ciberataques como la suplantación de identidad, el acceso a sus cuentas sin su consentimiento y la difusión o publicación de información secreta o íntima sin su consentimiento.

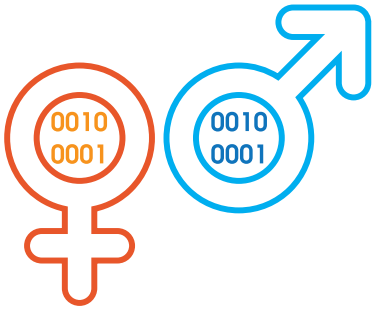
PUEDES AYUDARLES

Para evitar que pase…

- Explícale al menor los riesgos que conlleva publicar información privada o cedérsela a otras personas.
- Procura que la información privada de los menores sea guardada en dispositivos electrónicos no conectados a Internet como discos duros extraíbles o pen drives.
- Comunícale los peligros asociados a contactar con desconocidos en Internet.
- Revisa habitualmente los amigos agregados en sus perfiles de redes sociales.
- Intenta compartir con el menor el uso de Internet.

Si está pasando…

- Adviértele que no debe responder a insultos y/o provocaciones
- Ayúdale a bloquear y/o eliminar al contacto que esté molestándole.
- Guarda las pruebas del ciberacoso (mensajes insultantes, amenazantes, fotos manipuladas, etc.)
- Si son compañeros de la escuela, ponlo en conocimiento del equipo directivo del centro.
- Si los ataques persisten o son de especial gravedad, denúncialo a la policía.



CIBERACOSO SEXUAL

¿Qué es?

El término ciberacoso sexual engloba todas aquellas conductas delictivas que afectan a la libertad o a la libre formación sexual de los menores a través de Internet, pudiendo ir desde la obtención de pornografía, pasando por las amenazas hasta llegar a la proposición de un encuentro físico con la intención de llevar a cabo un abuso o agresión sexual.

Puede aparecer en forma de:

Online Grooming
También denominado "embaucamiento de menores" a través de Internet, consiste en la dinámica que utiliza un adulto para acercarse a un menor a través de las TIC y ganarse su confianza con la intención de solicitarle un encuentro sexual en el espacio físico.

"Hostigamiento sexual"
Son aquellas conductas en las que se aprovecha cualquier situación de comunicación cotidiana para lanzar un mensaje de tipo sexual al menor, siendo percibidas por éste como molestas o no deseadas.

Sextorsión
Se produce cuando alguien tiene en su poder una imagen de carácter sexual de otra persona, obtenida con consentimiento o sin él, y la utiliza con el fin de extorsionar, dañar o sacar algún tipo de beneficio, aprovechando la situación de vulnerabilidad de la víctima.

Se manifiesta…

En el **online grooming**, el acosador, para atraer la atención del menor y llevar a cabo un acercamiento, se hace pasar por alguien interesante, pudiendo mentir sobre su nombre y edad. Su intención es establecer una relación de confianza con el menor y conseguir que le envíe fotos con contenido sexual o se muestre frente a la webcam desnudo o semidesnudo. Posteriormente, le chantajea con hacer públicas las imágenes enviadas con el fin de citarse físicamente con él y llevar a cabo un abuso o agresión sexual.

A pesar de llevarse a cabo generalmente por hombres de edad adulta, también puede ser realizado por menores de edad, mujeres, o por alguien conocido (bien del entorno escolar, familiar o cualquier otro ámbito, incluso la propia pareja). En cualquier caso, la finalidad del ciberacosador es la búsqueda de satisfacción sexual.

La **sextorsión**, tiene como origen, generalmente, el sexting que consiste en el envío voluntario de material erótico o sexual a través de las TIC. El problema viene cuando la persona que tiene en su poder la imagen la utiliza para chantajear a la víctima bajo la amenaza de hacerla pública con la intención de mantenerla intimidada ante tus peticiones.

El **“hostigamiento sexual”** son comportamientos que suelen empezar como inofensivos y que acaban afectando a la dignidad del menor. Se manifiesta, sobre todo, a través de conductas como ser acosado con mensajes reiterativos de carácter sexual, peticiones sexuales a través de las redes sociales o chats, o recibir imágenes sexuales no deseadas. Puede llevarse a cabo en entornos semipúblicos (foros, chats, etc.) por parte de cualquier persona, desconocida o conocida, ya sea menor o adulto.

Es importante saber que…

El sexting es generalmente el punto de inflexión para una sucesiva sextorsión por lo que se considera una conducta de riesgo. Se da con relativa frecuencia entre nuestros menores, iniciándose muchas veces como un juego privado entre la víctima y un único destinatario (generalmente la pareja). En la provincia de Alicante, 1 de cada 10 menores de entre 16 y 18 años, envían de forma voluntaria vídeos y fotografías con contenido erótico o sexual a través del teléfono móvil, tablet u ordenador.

El alcance del fenómeno es…

Aproximadamente, el 6 % de los menores entre 12 y 18 años han sufrido alguna forma de ciberacoso sexual en algún momento de su vida. Haber sido acosado de forma reiterada con mensajes de carácter sexual a través de Internet o del teléfono móvil es la forma más frecuente, hecho que sufren especialmente las chicas. También son ellas las que tienen el doble de probabilidad de verse obligadas a enviar fotografías de naturaleza sexual.

Las consecuencias son…

Puede llegar a afectar al desarrollo psicosocial y sexual de la víctima, generar creencias erróneas o hábitos insanos sobre el sexo, incluso desarrollar una sexualidad prematura si es sufrida por menores de corta edad. Además, puede generar depresión, aislamiento y dificultad para relacionarse adecuadamente con otros menores.

Los que tienen más riesgo de sufrir estos ataques son…

Los menores alicantinos usuarios de redes sociales, foros y blogs que contactan con desconocidos y facilitan información personal. Además, los menores que no comparten el ordenador con otras personas, como padres y hermanos, así como los que guardan información personal (fotos personales o íntimas, vídeos, etc.) en el terminal desde al que se accede a Internet, tienen más probabilidad de convertirse en víctimas.

El menor tiene…

De 12 a 13 años

Al ser el grupo de edad más joven son más vulnerables a sufrir coacciones para realizar comportamientos de tipo sexual frente a la webcam. Su corta edad no le proporciona los recursos necesarios para afrontar situaciones amenazantes que les hagan sentir obligados a realizar estas conductas. Es, por ello, importante informar al menor de los peligros a los que se expone a través de las nuevas tecnologías y enseñarles a negarse frente a peticiones sexuales.

De 14 a 15 años

Son los menores con menor probabilidad de sufrir este tipo de ciberacoso, pero es importante tener en cuenta que a esta edad comienzan a establecer sus primeras relaciones íntimas y pueden llegar a realizar conductas más arriesgadas, como el sexting. Por tanto, es necesario recordarles la trascendencia de preservar su imagen y las consecuencias que puede tener enviar imágenes sexuales a través del móvil o Internet.

De 16 a 18 años

A esta edad, aumenta la probabilidad de sufrir ciberacoso sexual, especialmente el acoso repetido con mensajes de carácter sexual, además de sentirse obligados a enviar fotos de contenido sexual a través de Internet o el móvil.
Estos ataques son realizados, principalmente, por parte de desconocidos, aunque también pueden ser llevados a cabo por conocidos ajenos al colegio y por la pareja o ex pareja.
Es importante que comprendan el riesgo de aceptar como "amigos" a desconocidos en las redes sociales, así como chatear o contactar con ellos. Además, la percepción de madurez que el menor tiene sobre sí mismo a esta edad, conlleva que asuma más conductas de riesgo, como conocer gente nueva a través de las TIC y realizar sexting.

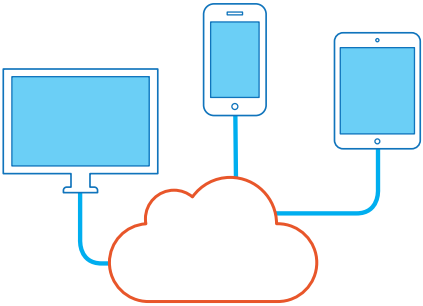
PUEDES AYUDARLES

Para evitar que pase…

- Enséñale que no debe guardar información personal en el ordenador y/o teléfono móvil desde el que conecta a Internet.
- Adviértele de que conocer a alguien a través de Internet conlleva el riesgo de que la persona no sea quien realmente dice ser o de que sus intenciones no sean las esperadas, por lo que no debe enviar información con la que le puedan chantajear.
- Tampoco debe facilitar información personal, especialmente fotos, el número de teléfono, el nombre completo, etc.
- Adviértele del peligro abrir enlaces o descargar archivos enviados de procedencia extraña o desconocida.
- Hazle saber la importancia de no acceder a propuestas sexuales a través de Internet (ni siquiera de la pareja).
- Recuérdale que enviar fotos y/o vídeos con contenido sexual de forma voluntaria, conlleva un riesgo real, puesto que perdemos el control de todo el contenido que se sube a Internet. Debe ser cauto con las fotos que envía o publica ya que le podrían chantajear para mandar más.
- Avísale que difundir imágenes de menores sin su consentimiento es un delito.
- Recomiéndale eliminar o bloquear a contactos o usuarios sospechosos.

Si está pasando…

- Aconséjale no ceder ante los chantajes o amenazas.
- Anímale a pedir ayuda a un adulto de confianza.
- Insístele en la importancia de guardar las pruebas del acoso (mensajes de amenaza, imágenes del acosador, etc.)
- Recomiéndale bloquear al acosador, eliminarlo y denunciarlo en la red social.
- Denúncialo a la policía.



CONTROL DE LA PAREJA

¿Qué es?

Se considera control de pareja aquellas conductas en la que uno de los miembros de la pareja, a través de Internet, en particular de las herramientas de comunicación que proporciona (como las redes sociales, las aplicaciones de mensajería instantánea, etc.) controla o manipula al otro para que se comporte de una determinada manera en el ciberespacio o fuera de él.

Este tipo de actos pueden presentarse de forma puntual, como pequeñas muestras de control que se manifiestan a través de las TIC, pero que pueden reproducirse también en el espacio físico. Sin embargo, el control de la pareja y de lo que ésta hace en el ciberespacio de forma continuada puede representar la existencia de otras formas de dominación posteriores y que revisten mayor gravedad.

Se manifiesta…

Por medio de múltiples acciones, como por ejemplo controlando las horas de conexión, las fotos que publica, los amigos o contactos que agrega en las redes sociales o vigilando con quien chatea. Otras formas en las que se manifiesta este dominio es mediante la obligación de retirar o poner fotos y/o publicaciones, exigir las contraseñas de las cuentas personales para acceder y supervisarlas o la imposición de la activación del geolocalizador para conocer su ubicación en todo momento. Estas conductas pueden ser una expresión de determinadas dinámicas de control machista.

El alcance del fenómeno es…

Aproximadamente, el 18 % de los menores alicantinos de edades entre 12 y 18 años ha sufrido alguna forma de control por parte de su pareja a lo largo de su vida, sobre todo, las chicas de entre 16 y 18 años. El control sobre los amigos o contactos que se agregan o eliminan en las redes sociales es una de las conductas más sufridas.

Es importante saber que…

Las relaciones sentimentales de dominio-sumisión cada vez se producen con mayor frecuencia entre los menores, potenciadas por el uso diario de las nuevas tecnologías, que permiten conductas de control directo sobre la pareja a través de las redes sociales, la mensajería instantánea, etc.

Las consecuencias son…

Puede desarrollar miedos irracionales, baja autoestima, aislamiento social y anulación de la personalidad. El dominio ejercido por el agresor a través de las TIC puede derivar en que la víctima cambie su estilo de vida, pierda poco a poco el criterio para tomar decisiones e incluso aumente su vulnerabilidad frente a una posible agresión física.

El menor tiene…

De 12 a 13 años

Al ser una edad aún temprana para tener relaciones de pareja son, en comparación con el resto de menores alicantinos, los que menos sufren este tipo de ciberataque. A pesar de ello, también existe un pequeño porcentaje que sufre control de su pareja a esta edad, por lo que conviene comenzar a hablar con el menor sobre las relaciones de pareja y explicarle qué conductas son apropiadas y cuáles no, para que no las sufran, pero también para que no las lleven a cabo. Las chicas sufren con mayor frecuencia que los chicos el control sobre los amigos que se agregan a las redes sociales o el teléfono móvil.

De 14 a 15 años

Algunos menores ya establecen relaciones de pareja a esta edad. Ciertas acciones pueden ser interpretadas erróneamente, creyendo el menor victimizado que se trata de pruebas de amor, llegando a considerar "lógicas" algunas conductas como ejercer control sobre los amigos agregados a las redes sociales o al teléfono móvil, o controlar qué fotos publica el menor. Así, uno de cada diez menores alicantinos de esta edad, sin distinción de sexo, sufren este tipo de control.

De 16 a 18 años

Las primeras relaciones de pareja comienzan a establecerse especialmente a estas edades, por este motivo el número de víctimas es mayor. El control de pareja se suele dar a través de la prohibición de contactar con determinadas personas o establecer restricciones para añadir o agregar a "amigos" a las redes sociales u otras aplicaciones de mensajería instantánea.

La preocupación excesiva por lo que pueda pensar la pareja y por las posibles represalias ante acciones cotidianas como agregar amigos o conocidos en las redes sociales, cambiar la foto de perfil o publicar contenido, son algunas de las manifestaciones que pueden observarse en aquellos menores que sufren el control de la pareja.

PUEDES AYUDARLES

Para evitar que pase…

- Si el menor tiene una relación sentimental, ínstale a establecer relaciones de pareja sanas, fundadas en la confianza y el respeto.
- Hazle saber que las muestras de control o los celos no son pruebas de amor.
- Establece un vínculo de confianza para hablar sobre las relaciones amorosas.
- Utiliza la comunicación como herramienta útil para prevenir malos hábitos en las relaciones de pareja. Para educar en igualdad no hay una edad, por lo que es importante enseñarles a respetar y tratar de forma igualitaria desde la infancia.
- Enséñale a no tolerar comportamientos inadecuados en el ciberespacio, igual que no se deben admitir en la vida real. Traslada la educación que le das en el espacio físico también al espacio virtual.

Si está pasando…

- Las conductas de control de pareja son una forma de violencia psicológica que podrían agudizarse y llegar a convertirse en violencia física, anímale a no tolerar esos comportamientos.
- Anímale a hablar con su pareja y hacerle comprender que las conductas de control son estrategias insanas que no tienen nada que ver con el amor.
- Si el control no cesa, ayúdale a plantearse la posibilidad de dejar esa relación.

CIBERFRAUDE ECONÓMICO

¿Qué es?

El término ciberfraude engloba todos los ataques que son realizados en el ciberespacio y que tienen como finalidad obtener un beneficio económico de manera ilícita.

Este tipo de acciones no siempre se lleva a cabo de manera directa, por ello debemos diferenciar entre el **robo de datos**, destinado a obtener información con el fin de llevar a cabo un posterior fraude económico y el **ciberfraude** propiamente dicho, en el que mediante una única acción se consigue el beneficio económico.

Se manifiesta…

En el **fraude en compra** hay un aprovechamiento de un contrato de compra-venta a través de Internet, que se traduce en que el vendedor cobra el producto pero nunca llega a enviarlo al comprador o envía un producto de una calidad inferior a la ofrecida.

La **Infección por virus o malware** hace referencia a los programas (software) que tienen como objetivo dañar el sistema informático eliminando o modificando archivos, obtener información, conseguir el control del sistema, etc. Aunque se suele hablar de virus, existen muchos tipos con funciones específicas como por ejemplo los gusanos, troyanos, keystroke loggers, etc.

El **Scam** consiste en enviar mensajes a los usuarios, generalmente a través del correo electrónico, redes sociales, mensajería instantánea, etc. en la que se prometen grandes cantidades de dinero a cambio de pequeñas transferencias relacionadas con la lotería, trabajo, etc.

El **Spam** es el envío masivo de correos electrónicos no deseados de publicidad, que en muchos casos son aprovechados por los hackers para enviar virus y contagiar un gran número de sistemas informáticos.

El **Phishing** consiste en el robo de datos personales, de la tarjeta de crédito o cuenta bancaria mediante diferentes técnicas como: correos electrónicos que llevan a páginas falsas en las que se solicita la introducción de estos datos, o mediante infección por virus.

Es importante saber que…

Podemos distinguir entre los ataques económicos mediales y los ataques económico puros o finales. Esta distinción es debía a que un hacker, para que lleve a cabo un ciberataque que obtenga un beneficio económico, es necesario que realice una cadena de ataques. Por ejemplo, el envío de spam suele el método para enviar un virus a un terminal para su posterior infección, que permita al hacker acceder a los datos identificativos del usuario y los de su tarjeta con los que, a continuación, realizar compras.

El alcance del fenómeno es…

Casi el 80% de los menores alicantinos entre 12 y 18 años, ha sufrido alguna forma de ciberfraude en algún momento de su vida. La forma más habitual es a través de la infección de algún tipo de virus, con un 74%. También es habitual por parte de los menores la recepción de correos electrónicos no deseados. En concreto, dos de cada diez de los jóvenes de la provincia ha recibido correos de scam y un 19% correos de spam. El porcentaje de menores que ha sufrido algún tipo de fraude en compra es del 4,4%.

Los que tienen más riesgo de sufrir estos ataques son…

Los menores que introducen en el ciberespacio datos personales reales para abrir cuentas en redes sociales o que facilitan sus contraseñas. También tienen más riesgo los menores que contactan con desconocidos a través de Internet y los que abren enlaces o descargan archivos enviados por desconocidos. Finalmente, los menores que reciben control por parte de sus padres sobre las horas y uso de Internet, tienen menos probabilidad de sufrir este tipo de victimización.

El menor tiene…

De 12 a 13 años

El ataque más común que sufren a esta edad es la infección por virus informático y la pérdida de archivos que éste conlleva, si bien es el grupo de menores con la tasa más baja en ciberfraude económico.

De 14 a 15 años

Los ciberataques que se sufren principalmente a esta edad son el fraude destinado a conseguir un beneficio económico bajo falsas promesas (scam), la publicidad masiva no solicitada (spam) y la infección y pérdida de archivos por virus informáticos.

De 16 a 18 años

Es el grupo con mayor número de víctimas en este tipo de ataques debido, principalmente, a que tienen mayor libertad para navegar por Internet con el ordenador y el teléfono móvil. Además de la infección por malware y de recibir correos de spam y/o de scam, son los que sufren un mayor ciberfraude en compra.

PUEDES AYUDARLES

Para evitar que pase…

- Enséñale a no abrir enlaces ni descargarse archivos enviados por desconocidos.
- Recuérdale que no debe fiarse de ofertas tentadoras o premios gratis ofrecidos por Internet.
- Háblale de la importancia de no facilitar sus contraseñas por Internet y de que debe cambiarlas con frecuencia.
- Aconséjale no realizar descargas de webs poco fiables. Puede comprobar la fiabilidad de la web recurriendo a webs o foros de opinión y verificando que usan el sistema de seguridad SSL fácilmente identificable verificando que la dirección comienza web comienza con "https".
- Hazle saber que cuando reenvíe un correo debe borrar las direcciones que aparecen y poner los correos en Copia Oculta (CCO) si lo van a enviar a varias personas.
- Supervisa y haz de manera conjunta las compras online que quiera realizar el menor.
- Consulta con tu banco o con el del menor qué sistemas ofrecen para realizar compras seguras por Internet como, por ejemplo, la tarjeta virtual.
- Evita que salgan ventanas emergentes, banners y anuncios poco apropiados mientras navega en Internet, instalándoles bloqueadores y filtros gratuitos disponibles en Internet.
- Comprueba que el antivirus está actualizado y funciona correctamente.

Si está pasando…

- Si el ordenador está infectado por un virus, compra e instala un antivirus o descárgalo de Internet y analiza el contenido del ordenador. También existen antivirus para los teléfonos móviles y las tablets.
- Ante el envío masivo de correos electrónicos no deseados, instala un filtro de seguridad en tu email.
- Cambia la contraseña de acceso de las cuentas de correo y de las redes sociales si consideras que ha podido ser infectada por un virus o por un hacker.
- Si al hacer una compra online no recibes el producto o no se corresponde con el artículo comprado, denúncialo. También debes denunciar si el importe cobrado por el vendedor no se corresponde con el precio de la compra.

CÓMO PREVENIR EN 20 SENCILLOS PASOS

1 No guardar información personal en los dispositivos conectados a Internet

Porque cuando guardamos toda nuestra información en los dispositivos que usamos para acceder al ciberespacio pasan a estar disponibles para potenciales agresores. Una forma sencilla de evitar riesgos es guardar toda la información en discos duros extraíbles o pendrives y hacer uso de ellos cuando no se está conectado a Internet, especialmente si se trata de información delicada o personal (fotos, cuentas y contraseñas bancarias, etc.)

2 No usar los datos personales reales

Especialmente para abrir cuentas de correo electrónico, perfiles en redes sociales, chats, blogs o webs de descarga, porque los datos pasan a estar disponibles para otras personas, incluso para quien no queremos que lo esté. Omite los campos que no son obligatorios para llevar a cabo el registro y excepto en páginas de organismos oficiales o de entidades bancarias, es recomendable utilizar un apodo con el que solo el círculo cercano le pueda identificar.

3 No facilitar información personal o íntima a otras personas a través de Internet

Porque cuando cedemos nuestra información personal, como fotos, vídeos o contraseñas a otras personas, aunque sean conocidas o de confianza, a través de mensajería instantánea, redes sociales, correo electrónico, etc. perdemos el control de esa información.

Los menores deben saber la importancia de preservar su intimidad y de que sus imágenes o datos pueden ser utilizadas por otras personas sin su consentimiento. Hazles reflexionar sobre cómo se sentirían si la información que va a publicar o a enviar a otra persona fuese difundida sin su consentimiento en Internet.

4 Evitar el contacto con desconocidos

Porque aceptar peticiones de amistad de extraños en las redes sociales, establecer contacto a través de otras vías como videojuegos, chats, blogs o aplicaciones de mensajería instantánea puede aumentar el riesgo de sufrir algún tipo de ciberacoso. Recomiéndale al menor que elimine de sus contactos a aquellas personas que no conoce o con las que no tiene amistad. También es recomendable evitar abrir enlaces o descargar archivos de origen desconocido para prevenir algunas formas de ciberfraude.

5 Debes estar al día con la tecnología ...

Porque a pesar de que no necesites ser un experto, conocer las novedades y manejar a nivel usuario las distintas herramientas que usan los menores facilita la comunicación con ellos y permite compartir espacios virtuales. Ellos mismos pueden ser nuestros maestros, de este modo lograrás acercarte más al nivel de manejo que él tiene y a los instrumentos que utiliza en Internet.

6 Hacer usos de sistemas de control parental o filtros

Puede ser una forma útil de restringir el acceso a páginas web con contenidos no apropiados para el menor. La instalación de estos programas en los dispositivos de los menores es muy sencilla y también nos puede permitir limitar el acceso en diferentes franjas horarias, registrar las páginas web visitadas, etc.

7 Supervisa la configuración de privacidad de sus perfiles en las redes sociales

Ya que existen diferentes opciones a la hora de compartir la información publicada, pudiendo ser desde completamente abiertas, a ser visibles para amigos de los amigos, o accesibles sólo para las personas seleccionadas y sólo para uno mismo.

Es recomendable restringir las publicaciones y fotos para que sólo puedan ser vistas por los contactos agregados a su lista de amigos o algún grupo en particular. También se debe comprobar periódicamente la privacidad de los perfiles puesto que la red social puede cambiar la configuración general de la aplicación sin que sepamos que ha cambiado nuestro criterio de privacidad.

8 Mantener actualizados los antivirus, cortafuegos y sistemas operativos del dispositivo desde el que accede a Internet…

Favorece la protección contra virus informáticos. También es recomendable actualizar los navegadores desde los que se accede a Internet.

9 Compartir el ordenador, portátil o tablet desde el que accede a Internet

Ya que podremos hacer un control de las descargas, de la actualización de los sistemas de protección, de las páginas visitadas, etc. Además, ubicar el ordenador en una zona común de la casa es también un buen recurso para controlar el uso que hacen de él.

10 Dedícale tiempo y espacio al menor y al uso que hace de las TIC

Puesto que es muy importante fomentar la comunicación entre los menores y los educadores. Pregúntale cuál es su actividad favorita en Internet o qué es lo que hace de forma habitual, sin ser intrusivo y mostrando confianza. Son buenas estrategias para acercarse al manejo que hacen los menores de las TIC y establecer normas y límites consensuados sobre el tiempo o forma de uso.

11 Enséñale a respetar las opiniones publicadas y a comunicarse de forma respetuosa

Pues un comportamiento irrespetuoso tiene efectos dañinos en otras personas y también puede ser causa de que sea acosado como respuesta a ese comportamiento.

12 No continuar las cadenas de correos electrónicos

Porque al reenviarlos, enviamos la dirección de nuestros contactos, favoreciendo que se puedan realizar envíos masivos de correos fraudulentos. Por ello, es importante que al mandar correos electrónicos pongamos como Copia Oculta (CCO) a los destinatarios.

13 Realizar copias de seguridad de los documentos y archivos de forma periódica

Con el fin de evitar la pérdida de los mismos en el caso de infección por virus malicioso del ordenador, tablets y teléfono móvil.

14 Evita entrar en páginas poco seguras

Para ello confirma que las páginas en las que se requiere información delicada deben tener un mecanismo de seguridad llamado SSL. Podemos identificar que este mecanismo de seguridad está habilitado cuando observamos en nuestro navegador que el sitio inicia con "**https**". Esa "**s**" significa que la comunicación entre el sitio y nuestro navegador va cifrada, es decir, protegida. Otra señal de que estamos en una web segura es que se encienda un candado en el navegador.

15 No confíes en promociones ni aceptes obsequios fáciles de obtener a través de Internet...

Ya que a través de ellos los agresores obtienen datos personales que pueden utilizar sin nuestro consentimiento. Podemos recibir las promociones a través del correo electrónico, mensajería instantánea o redes sociales.

16 A la hora de realizar compras online es importante usar métodos seguros

Como por ejemplo las tarjetas virtuales o de prepago, puesto que nos permiten poner la cuantía exacta destinada únicamente a la compra que vamos a realizar, evitando que nuestros datos puedas ser grabados y utilizados con posterioridad para hacer compras sin nuestra autorización.

17 Utiliza contraseñas seguras

Para evitar que puedan ser descifradas. Es importante no utilizar la misma contraseña de acceso para todas las cuentas, y que nuestras contraseñas contengan más de 8 dígitos, alternando mayúsculas, minúsculas, números y símbolos.

18 No todo lo que vemos publicado en Internet es cierto

Por lo que es importante enseñar al menor a contrastar información para evitar que pueda ser engañado.

19 Desconecta o tapa la webcam cuando no se esté usando

Porque mediante malware pueden controlar nuestros sistemas informáticos con los que accedemos a Internet, teniendo posibilidad de grabarnos sin darnos cuenta y hacer públicos esos archivos. Es recomendable poner una pegatina sobre la cámara si se trata de una webcam integrada (como en ordenadores portátiles o tablets) ya que es una forma sencilla de prevenir este tipo de ciberataques.

20 Ser cuidadoso al acceder a Internet desde ordenadores o dispositivos móviles públicos o hacer uso de redes WiFi abiertas

Ya que pueden obtener nuestros datos y ser utilizados para fines ilegales. Se recomienda al hacer uso de estos sistemas no utilizar cuentas personales y fijarnos en no seleccionar la opción "recordar nombre o contraseña". Debemos asegurarnos de cerrar la sesión y que no queden grabados los datos introducidos.

MEDIOS DE APOYO

PROGRAMAS DE SEGURIDAD Y CONTROL

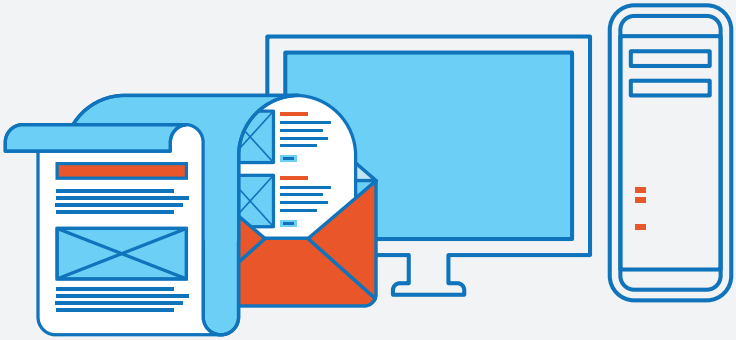
Tenemos a nuestra disposición varios programas informáticos destinados a controlar el uso que se hace de Internet, bloquear las posibles amenazas y preservar la privacidad y seguridad de nuestros equipos.

www.controlkids.com
Control Kids es un programa de control paterno que filtra todo contenido inadecuado de los sitios web: la pornografía, la violencia, la pedofilia, las sectas religiosas, los sitios de descargas ilícitas, etc.

www.qustodio.com
Qustodio bloquea el contenido peligroso y permite visualizar la actividad social de tu hijo en las redes sociales. Además permite establecer límites de uso.

www.kidbox.net
Kidbox es una herramienta segura que bloquea la publicidad y los enlaces no deseados. La interfaz se convierte en la única vía de acceso a Internet donde el menor tiene su propia lista de contactos aprobados y gestionados por el adulto.

www.adblockplus.org
Adblock permite bloquear y ocultar elementos publicitarios molestos de las páginas web al navegar por Internet.

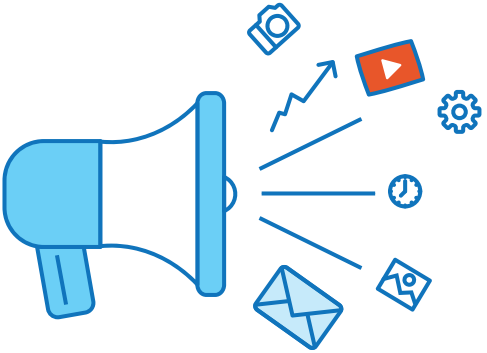


RECURSOS INFORMATIVOS

Existen webs que presentan material didáctico y todo tipo de información referente al uso que hacen los menores de las nuevas tecnologías. Resultan de gran utilidad para preservar su seguridad en el ciberespacio y estar al día de las nuevas formas de ciberataque.

La Oficina de Seguridad Internauta (OSI www.osi.es) y el **Instituto Nacional de las Tecnologías de la Comunicación** (INTECO www.inteco.es) proporcionan soporte para evitar y resolver los problemas de seguridad que pueden existir al navegar por Internet.

Patallas Amigas (www.pantallasamigas.net) y **Protégeles** (www.protegeles.com) fomentan el uso seguro y responsable de las nuevas tecnologías en niños y adolescentes. Ofrecen apoyo, recursos didácticos e informativos, noticias y servicios de denuncias.



WEBS DE DENUNCIA

No lo permitas, ¡actúa!

Si está sufriendo algún tipo de ciberacoso, no estáis solos. **Denunciar es la mejor opción**, por ello es importante guardar las pruebas. No borres los mensajes, fotos, audios o vídeos que prueben el acoso que el menor está sufriendo. Guarda todo aquello que identifique al ciberacosador y que demuestre la veracidad de tu denuncia.

Los Cuerpos y Fuerzas de Seguridad del Estado ofrecen dos vías para realizar denuncias online:

- Oficina virtual de denuncias del CNP: **https://denuncias.policia.es**
- Brigada de Investigación Tecnológica: **www.policia.es/bit**
- Grupo de delitos telemáticos Guardia Civil: **www.gdt.guardiacivil.es**

También puedes denunciar a través de:

Protégeles tiene una "línea de denuncia" para alertar sobre webs con contenido ilegal: **www.protegeles.com**

CIBERAPP

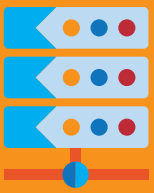
Aprender
Prevenir
Proteger

Prevenir

Aprender

Proteger

CIBERAPP



CRÍMINA
Centro para el estudio y prevención de la delincuencia

UNIVERSITAS Miguel Hernández

DIPUTACIÓN DE ALICANTE